UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/769,844	01/25/2001	Joseph C. Kawan	CITI0212	5508

27510 7590 05/25/2005

KILPATRICK STOCKTON LLP
607 14TH STREET, N.W.
WASHINGTON, DC 20005

EXAMINER	
NGUYEN, MINH DIEU T	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/769,844	KAWAN ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-91* is/are pending in the application.

4a) Of the above claim(s) *18,28,63 and 73* is/are withdrawn from consideration.

5)☒ Claim(s) *30 and 75* is/are allowed.

6)☒ Claim(s) *1-17,19-27,29,31-38,40-44,46-62,64-72,74,76-83,85-89 and 91* is/are rejected.

7)☒ Claim(s) *39,45,84 and 90* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication dated February 7, 2005 with the amendments to claims 1-7, 12, 22-23, 29-30, 46-52, 57, 67-68, 74-75 and 91 and the cancellation of claims 18, 28, 63 and 73.

Claims 1-91 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-91 have been considered but are moot in view of the new ground(s) of rejection. Applicant's arguments focus on the combination of features introduced by the amendment with elements that already existed in the claims. The new material is rendered obvious by Piosenka et al. (4,993,068) and Kanevsky et al. (6,421,453).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-17, 19-27, 29, 31-38, 40-44, 46-62, 64-72, 74, 76-83, 85-89 and 91 are rejected under 35 U.S.C. 103(a) as being unpatentable over Piosenka et al. (4,993,068) in view of Kanevsky et al. (6,421,453).

a) As to claims 1, 46 and 91, Piosenka discloses a personal identification system for identifying users at remote access control sites comprising the steps of enrolling a plurality of credentials for the user with the authority (Fig.1, col. 4, lines 2-21); establishing at least one shared secret between the user and the authority relating to a predefined shared secret manner for presenting a current user credential to the authority (col. 9, lines 22-25); receiving at least one currently presented user credential by the authority for authentication of the identity of the user (col. 8, lines 33-35) and authenticating an identity of the user by the authority based on a correspondence between the enrolled and current user credentials (col. 8, lines 50-58) and a correspondence between the shared secret manner for presenting the current user credential and the manner in which the current user credential is presented to the authority (col. 5, lines 6-19).

Piosenka discloses the shared secret manner allowing the authentication process to be performed with higher accuracy and security, for example, at a point of sales terminal, facial feature biometric and financial attribute data are required, however at the guard station of a military base, perhaps both facial information and the fingerprint biometric are needed (col. 9, lines 50-64), however Piosenka does not disclose a predefined shared secret manner for presenting each of a plurality of current user credentials to the authority for the user for consecutive occasions.

Kanevsky discloses a predefined shared secret manner for presenting each of a plurality of current user credentials (i.e. acoustic and non-acoustic features, such as voice characteristics and answers to random questions) to the authority for the user for consecutive occasions (col. 11, lines 30-57).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a predefined shared secret manner for presenting each of a plurality of current user credentials to the authority for the user for consecutive occasions in the system of Piosenka, as Kanevsky teaches so as to accurately and securely authenticate users .

b) As to claims 2-3 and 47-48, Piosenka discloses the method wherein enrolling the user credential further comprises receiving and storing the plurality of user credentials by the authority (Figure 1, element 40).

c) As to claims 4-6 and 49-51, Piosenka discloses the method wherein storing the plurality of user credentials further comprises storing at least one biometric template for the user (Fig. 1, element 13); storing at least one document for the user (Fig. 1, element 10); storing the plurality of user credentials on one of a host computer, a local terminal, and a smart card for the user (col. 6, lines 40-54).

d) As to claims 7-11 and 52-56, Piosenka discloses the method wherein enrolling the plurality of user credentials further comprises enrolling at least one biometric template for at least one of a fingerprint, a face, a voice and an iris template (Fig. 1, elements 11-15) and at least one document further comprises at least one of a digital document comprising at least one of a digital certificate and a digital signature

and a paper document comprises a passport for the user (Fig. 1, element 10; col. 1, lines 56-58; col. 5, lines 32-50; col. 7, lines 12-17).

e) As to claims 12-13 and 57-58, Piosenka discloses the method wherein enrolling the plurality of user credentials with the authority further comprises storing user authentication information on a user token, on a smart card (col. 6, lines 40-47).

f) As to claims 14-15 and 59-60, Piosenka discloses the method wherein storing the information on the smart card further comprises storing biometric information having one of a fingerprint, a face, a voice and an iris for the user (Fig. 1, elements 11-14, 40).

g) As to claims 16 and 61, Piosenka discloses the method wherein storing the information on the smart card further comprises storing the shared secret for the user (col. 9, lines 22-25).

h) As to claims 17 and 62, Piosenka discloses the method wherein storing the information on the smart card further comprises storing the authentication information on the smart card signed with a private key for the user (col. 5, lines 52-64).

i) As to claims 19-20 and 64-65, Piosenka discloses predefined shared secret manner, he does not disclose the predefined shared secret sequence of presenting the current user credential to the authority.

Kanevsky et al. discloses the methods and apparatus for user recognition (classification/identification/verification) to grant access or service to authorized users especially to methods and apparatus for providing same employing gesture and speaker recognition by pre-storing a predefined sequence of intentional gestures

performed by the individual during an enrollment session; extracting the predefined sequence of intentional gestures from the individual during a recognition sessions and comparing the pre-stored sequence to the extracted sequence to recognize the individual; the predefined shared secret sequence which functions in a manner analogous to a personal identification number for the user (col. 3, lines 27-37)

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of predefined shared secret sequence in the system of Piosenka, as Kanevsky teaches, so as to improve the accuracy and security in authenticating users.

ji) As to claims 21 and 66, Piosenka discloses the method wherein establishing the shared secret further comprises storing information about the shared secret by the authority (col. 9, lines 22-27).

k) As to claims 22-23 and 67-68, Piosenka discloses the method wherein storing the information about the shared secret further comprises storing the information about the encrypted and digitally signed shared secret and the plurality of user credentials together in a database by the authority (col. 6, lines 32-54).

l) As to claims 24-26 and 69-71, Piosenka discloses the method wherein establishing the shared secret further comprising establishing at least one additional shared secret comprising a predefined shared secret personal identification number between the user and the authority; establishing at least one additional predefined shared secret manner of presenting the current user credential to the authority (col. 9, lines 22-31).

m) As to claims 27, 29, 72 and 74, Piosenka discloses the method wherein establishing the additional shared secret further comprises establishing a predefined shared secret manner of presenting at least one additional current user credential to the authority (col. 9, lines 50-64); of presenting each of a plurality of additional current user credentials comprising establishing a variation of the predefined shared secret manner of presenting each of the additional current user credentials to the authority for the user corresponding to a variation in a degree of security (col. 9, lines 1-21).

n) As to claims 31, 36, 76 and 81, Piosenka discloses the authority receiving the current user credential; directing the user to present a combination of biometric samples for at least two of a user fingerprint, a user face, a user voice and a user iris in a predefined shared secret sequence (col. 9, line 50 to col. 10, line 3).

o) As to claims 32-33 and 77-78, Piosenka discloses the method wherein receiving the currently presented user credential further comprises receiving a current biometric sample having one of a fingerprint, a face, a voice and an iris for the user by the authority (Fig. 2, element 3; col. 8, lines 10-12, 33-47).

p) As to claims 34-35 and 79-80, Piosenka discloses the method wherein receiving the currently presented user credential further comprises receiving the current user credential in a shared secret manner directed by the authority (col. 9, lines 22-25); further comprising the user to present a biometric sample for at least one user fingerprint (Fig. 2, element 33) or to present a combination of biometric samples for at least two of a user fingerprint, a user face, a user voice and a user iris (col. 8, lines 33-47).

q) As to claims 37-38 and 82-83, Piosenka discloses the method wherein receiving the current user credential further comprises receiving at least one additional currently presented user credential by the authority and in a manner directed by the authority (col. 9, lines 50-64).

r) As to claims 40-41 and 85-86, Piosenka discloses the method wherein authenticating the identity of the user by the authority further comprises authenticating the identity of the user by one of a host computer and a local device (Fig. 2, elements 4 and 35) and authenticating the identity of the user for activation one of a gate controller, a door opener, a telephone and an appliance (col. 8, lines 6-9).

s) As to claims 42, 44, 87 and 89, Piosenka discloses the method wherein authenticating the identity of the user by the authority further comprises authenticating the identity of the user based on the enrolled user credential and the shared secret manner for presenting the current user credential stored together in one of a local database and a remote database of the authority (col. 9, lines 50-64; col. 6, lines 40-54).

t) As to claims 43 and 88, Piosenka discloses the method wherein authenticating the identity of the user in order for access to one of a device which activating a silent alarm, a physical location, he does not disclose accessing to a network.

Kanevsky discloses a method for controlling access of an individual to one of a computer and service and a facility (Abstract).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of authenticating users for accessing network in the system of Piosenka, as Kanevsky teaches, so as to provide more services to users.

Allowable Subject Matter

5. Claims 39, 45, 84 and 90 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

6. Claims 30 and 75 are allowed.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
5/17/05

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER